

IT Security Handbook

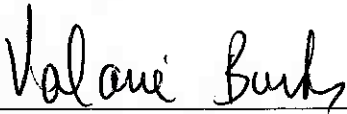
System and Information Integrity

ITS Handbook (ITS-HBK-2810.14-01)
System and Information Integrity

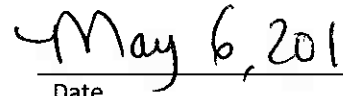
Distribution:

NODIS

Approved



Valarie Burks
Deputy Chief Information Officer for
Information Technology Security



Date

Change History

Version	Date	Change Description
1.0		Initial Draft

Table of Contents

Change History.....	3 -
1 Introduction and Background	5 -
2 Flaw Remediation (SI-2).....	5 -
3 Malicious Code Protection (SI-3)	6 -
4 Information System Monitoring (SI-4)	7 -
5 Security Alerts, Advisories, and Directives (SI-5)	8 -
6 Security Functionality Verification (SI-6)	8 -
7 Software and Information Integrity (SI-7).....	8 -
8 Spam Protection (SI-8)	8 -
9 Information Input Restrictions (SI-9)	8 -
10 Information Input Validation (SI-10).....	8 -
11 Error Handling (SI-11)	8 -
12 Information Output Handling and Retention (SI-12)	8 -
13 Organizationally Defined Values.....	9 -

1 Introduction and Background

- 1.1 - NASA requirements for protecting the security of NASA information and information systems are derived from National Institute of Standards and Technology (NIST) guidance. Information System Owners (ISOs) and other personnel responsible for the protection of NASA information or information systems shall follow NIST guidance in the proper security categorization (*Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization for Federal Information and Information Systems*), and in the selection and implementation of information security controls (*FIPS 200, Minimum Security Requirements for Federal Information and Information Systems* and *NIST Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems and Organizations*), in a manner consistent with the Risk Management Framework (*NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems*).
- 1.2 - This handbook augments NIST guidance by providing NASA-specific requirements, procedures and recommendations, where applicable. NASA-specific guidance does not negate NIST guidance, unless explicitly stated.
- 1.3 - *NASA Policy Directive (NPD) 2810.1, NASA Information Security Policy, NASA Procedural Requirements (NPR) 2810.1, Security of Information Technology*, and the collection of 2810 Information Technology Handbooks (ITS-HBK) satisfy the policy and procedure controls of *NIST SP 800-53, Recommended Security Controls for Federal Information Systems and Organizations*.
- 1.4 - *NPR 2810.1, Security of Information Technology*, designates this handbook as a guide of NASA's System and Information Integrity (SI) information security controls.
- 1.5 - The terms "shall" and "may" within this handbook are used as defined in *ITS-HBK-0001, Format and Procedures for IT Security Policies and Handbooks*.
- 1.6 - The System and Information Integrity control family relates to the prevention and detection of improper modification or destruction of an information system. The control family also includes ensuring the non-repudiation and authenticity of information, as well as flaw remediation (e.g., patching vulnerable software), malicious code prevention (e.g., anti-virus software), and monitoring of attempts to subvert integrity (e.g., an intrusion detection system).
- 1.7 - **Applicable Documents**
- *NPD 2810.1, NASA Information Security Policy*
 - *NITR 2810-24, NASA IT Device Vulnerability Management*
 - *NITR 2800-2, Email Services and Email Forwarding*
 - *NPR 2810.1, Security of Information Technology*
 - *ITS-HBK-0001, Format and Procedures for IT Security Policies and Handbooks*
 - *ITS-HBK-2810.04-01, Risk Assessment*
 - *FIPS 199, Standards for Security Categorization for Federal Information and Information Systems*
 - *FIPS 200, Minimum Security Requirements for Federal Information and Information Systems*
 - *NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems*
 - *NIST SP 800-40, Creating a Patch and Vulnerability Management Program*
 - *NIST SP 800-53, Recommended Security Controls for Federal Information Systems and Organizations*
 - *NIST SP 800-83, Guide to Malware Incident Prevention and Handling*
 - *NIST SP 800-94, Guide to Intrusion Detection and Prevention Systems*
 - *NIST SP 800-92, Guide to Computer Security Log Management*

2 Flaw Remediation (SI-2)

- 2.1 - **Roles and Responsibilities**
- 2.1.1 *The Senior Agency Information Security Officer (SAISO) shall:*
- 2.1.1.1 Provision an Agency-wide mechanism for the identification and reporting of information system patches.

ITS Handbook (ITS-HBK-2810.14-01) -
System and Information Integrity -

- 2.1.1.2 Designate patches for critical vulnerabilities of a particularly serious nature that pose a significant threat to the security posture of the Agency as “Expedited”.
- 2.1.2 *The Information System Owner (ISO) shall:*
 - 2.1.2.1 Ensure the remediation or mitigation of all vulnerabilities in accordance with *ITS-HBK-2810.04-01*.
 - 2.1.2.2 Ensure the automated capability to determine the state of information systems with regard to flaw remediation in a manner consistent with organizationally defined values.
 - 2.1.2.3 Ensure that all information system components are up-to-date with all applicable patches which may impact the security of information systems.
 - 2.1.2.4 Ensure the installation of Agency-approved patch management/reporting software agents on information systems which support the agent.
 - 2.1.2.4.1 Agents should be configured to automatically report patch status to the Information Technology Security Enterprise Data Warehouse (ITSec-EDW).
 - 2.1.2.5 When automation is not possible, ensure the registration of devices in ITSec-EDW, and report patch status manually by the second Monday of each month.
 - 2.1.2.6 Ensure that devices with patch management software agents are grouped by System Security Plan number (SSP) in ITSec-EDW.
 - 2.1.2.7 Ensure that any devices on NASA networks that continue to exhibit the same unmitigated or unaccepted vulnerabilities identified in three (3) consecutive monthly vulnerability scans are disconnected from the network, and only re-connected once all residual risks are accepted.
 - 2.1.2.7.1 Center Chief Information Officers (CIO), Center Chief Information Security Officer (CISO), Organization Computer Security Officials (OCSO), or ISOs may choose to disconnect devices sooner, depending on the severity of the vulnerabilities, or sensitivity of the device.
- 2.1.3 *The Information System Security Officer (ISSO) shall:*
 - 2.1.3.1 Test information system patches and updates prior to installation, in a manner commensurate with the level of risk.
- 2.1.4 *The Agency Security Update Service (ASUS) Project Manager shall:*
 - 2.1.4.1 Coordinate the management of the NASA patch management solution.
 - 2.1.4.2 Work with patch management administrators across the Agency to ensure patch management and reporting capabilities.
 - 2.1.4.3 Ensure that patch management baselines consist of all current vendor critical patches.
 - 2.1.4.4 Ensure the patch status of all information system devices on non-guest NASA networks are reported in ITSec-EDW.
 - 2.1.4.5 Provide the capability to report on expedited patch status and patch compliance on IT devices, based on automatically collected and Center-reported data.
 - 2.1.4.6 Provide the capability to report any information system devices recorded in ITSec-EDW that do not have patch management/reporting software agents installed, and that have not been registered manually.
 - 2.1.4.7 Provide the capability to report any information system devices recorded in ITSec-EDW that are not associated with an SSP.

3 Malicious Code Protection (SI-3)

3.1 Roles and Responsibilities

- 3.1.1 *The SAISO shall:*
 - 3.1.1.1 Define the acceptability of malicious code protection tools for use across the Agency.
- 3.1.2 *The ISO shall:*

System and Information Integrity

- 3.1.2.1 Ensure that Agency approved malicious code protection tools are installed on information systems that support the use of malicious code protection tools.
 - 3.1.2.1.1 Malicious code protection tools should be appropriate for the information systems on which they are installed.
 - 3.1.2.1.2 Malicious code protection tools should be employed at applicable Agency information system entry and exit points, as well as workstations, servers and/or mobile computing devices on the network.
- 3.1.2.2 Ensure only privileged users are able to make changes to malicious code protection tools, including the ability to skip updates or not scan files automatically.
- 3.1.3 *The ISSO shall:*
 - 3.1.3.1 Ensure that malicious code protection tools are automatically updated with new releases and signature definitions.
 - 3.1.3.2 Ensure that malicious code protection tools are configured to operate in a manner consistent with organizationally defined values.
 - 3.1.3.3 Ensure that false positives during malicious code detection and eradication are addressed regarding potential impact on the information system availability.

4 Information System Monitoring (SI-4)

4.1 Roles and Responsibilities

- 4.1.1 *The SAISO shall:*
 - 4.1.1.1 Define the acceptability of information system monitoring tools for use across the Agency.
 - 4.1.1.2 Provision the capability for intrusion monitoring and detection of NASA information systems.
- 4.1.2 *The Center CISO shall:*
 - 4.1.2.1 Ensure that information system monitoring tools are deployed strategically to collect information, and to track specific types of transactions of interest to the Agency, or Center.
 - 4.1.2.2 Ensure the level and intensity of information system monitoring is heightened whenever there are indications of increased risk based on creditable sources of information.
- 4.1.3 *The OCSO shall:*
 - 4.1.3.1 Ensure that information system monitoring tools are deployed strategically to collect information, and to track specific types of transactions of interest to the Agency, or organization.
 - 4.1.3.2 Ensure the level and intensity of information system monitoring is heightened whenever there are indications of increased risk based on creditable sources of information.
- 4.1.4 *The ISO shall:*
 - 4.1.4.1 Ensure information system monitoring tools and techniques are employed in a manner consistent with organizationally defined values.
- 4.1.5 *The ISSO shall:*
 - 4.1.5.1 Ensure that information system inbound and outbound communication is monitored for unusual or unauthorized activities or conditions.
 - 4.1.5.2 Ensure that the system prevents non-privileged users from disabling or altering intrusion detection prevention controls or monitoring.
 - 4.1.5.3 Report suspected or actual IT security incidents immediately to the Security Operations Center (SOC), Center CISO or other appropriate organizations (e.g., Center-specific IT security office, incident response team, or help desk).
 - 4.1.5.4 Report suspected or actual potential misuse activity, detected in the course of their duties, to the ISO, Center CISO, OCSO, SAISO, or other appropriate authority.

5 Security Alerts, Advisories, and Directives (SI-5)

5.1 - Roles and Responsibilities

5.1.1 *The SOC Operations Manager shall:*

- 5.1.1.1 - Ensure the SOC is the primary interface with the US-CERT and other outside agencies, and generates internal security alerts and advisories as necessary.
- 5.1.1.2 - Ensure that security alerts, advisories, and directives from external sources can be received on an ongoing basis.
- 5.1.1.3 - Ensure dissemination of information security alerts, advisories, and directives in a manner consistent with - organizationally defined values. -

6 Security Functionality Verification (SI-6)

6.1 - Roles and Responsibilities

6.1.1 *The ISO shall:*

- 6.1.1.1 - Ensure validation of information system security functionality in transitional states in a manner compliant with organizationally defined values.
- 6.1.1.2 - Ensure information systems react to anomalies in transitional states in a manner consistent with organizationally defined values.

7 Software and Information Integrity (SI-7)

7.1.1 *The ISO shall:*

- 7.1.1.1 - Ensure the reassessment of the integrity of software and information by performing integrity scans in a manner consistent with organizationally defined values.

8 Spam Protection (SI-8)

8.1 - Roles and Responsibilities

8.1.1 *The SAISO shall:*

- 8.1.1.1 - Define the acceptability of Agency-wide spam protection tools as applied by the NASA Operational Messaging and Directory Service (NOMAD).

9 Information Input Restrictions (SI-9)

- 9.1 - NIST guidance is the authoritative source for selection and implementation of this control based on the security categorization and risk environment of the information and/or information system.

10 Information Input Validation (SI-10)

- 10.1 - NIST guidance is the authoritative source for selection and implementation of this control based on the security categorization and risk environment of the information and/or information system.

11 Error Handling (SI-11)

11.1 - Roles and Responsibilities

11.1.1 *The ISO shall:*

- 11.1.1.1 - Ensure the identification of potential security-relevant information system error conditions in a manner consistent with organizationally defined values.

12 Information Output Handling and Retention (SI-12)

- 12.1 - NIST guidance is the authoritative source for selection and implementation of this control based on the security categorization and risk environment of the information and/or information system.

13 Organizationally Defined Values

The following table provides the values defined in *NIST SP 800-53* as being at the discretion of the implementing organization. The Section, and Parameter columns are intended to help navigate various *NIST SP 800-53* security controls for easier application of the organizationally defined values; these columns are defined as follows:

- Section: Values in this column indicate whether an organizationally defined value is in the main body of the control (Main), or part of one of the control's enhancements (E1, E2, etc).
- Parameter: Sometimes, a specific Section may have multiple organizationally defined values. In those instances, the bracketed number Parameters indicate which organizationally defined value (numbered sequentially) is being referenced. In the case of nested organizationally defined values, a series of bracketed numbers is used.

Family	#	Name	Section	Parameter	Type	Description	Low	Moderate	High
SI	01	System and Information Integrity Policy and Procedures	Main	[1]	Frequency	Policy and procedure review.	1/Year	1/Year	1/Year
SI	02	Flaw Remediation	E 2	[1]	Frequency	Use of automated mechanisms to determine the state of information system components with regard to flaw remediation.	1/Week	1/Week	1/Week
SI	02	Flaw Remediation	E 3	[1]	Reference	Benchmarks for comparison of time between flaw identification and flaw remediation.			
SI	02	Flaw Remediation	E 4	[1]	Reference	Information system components for which automated patch management tools are used.			
SI	03	Malicious Code Protection	Main	[1]	Frequency	Periodic scans of information systems for the detection of malicious code.	1/Week	1/Week	1/Week
SI	03	Malicious Code Protection	Main	[2]	Selection	Response to malicious code detection.	Organization defined action	Organization defined action	Organization defined action
SI	03	Malicious Code Protection	Main	[2] [1]	Reference	Organization defined action for response to malicious code detection.	Ensure incident response personnel are notified.	Ensure incident response personnel are notified.	Ensure incident response personnel are notified.
SI	03	Malicious Code Protection	E 6	[1]	Frequency	Testing of malicious code protection tools with benign, non-spreading test cases.			

ITS Handbook (ITS-HBK-2810.14-01) -
System and Information Integrity -

Family	#	Name	Section	Parameter	Type	Description	Low	Moderate	High
SI	04	Information System Monitoring	Main	[1]	Reference	Monitoring objectives for detection of system attacks.		(1) Detecting attack (2) Detecting unauthorized use (3) Identifying actions to mitigate the impact of attacks and unauthorized use	(1) Detecting attack (2) Detecting unauthorized use (3) Identifying actions to mitigate the impact of attacks and unauthorized use
SI	04	Information System Monitoring	E 5	[1]	Reference	Indications of potential compromise which trigger real-time alerts.		(1) Hit by Agency or Center prohibited IP addresses or domains (2) A security policy change	(1) Hit by Agency or Center prohibited IP addresses or domains (2) Privilege escalation (3) A security policy change
SI	04	Information System Monitoring	E 7	[1]	Reference	List of personnel to be notified of security alerts, advisories, and directives.			
SI	04	Information System Monitoring	E 7	[2]	Reference	List of least disruptive actions for termination of suspicious events.			
SI	04	Information System Monitoring	E 9	[1]	Time Period	Testing of intrusion-monitoring tools.			
SI	04	Information System Monitoring	E 12	[1]	Reference	List of unusual or inappropriate activities which trigger alerts.			
SI	04	Information System Monitoring	E 13	[1]	Reference	Measure of false positives.			
SI	04	Information System Monitoring	E 13	[2]	Reference	Measure of false negatives.			

ITS Handbook (ITS-HBK-2810.14-01) -
System and Information Integrity -

Family	#	Name	Section	Parameter	Type	Description	Low	Moderate	High
SI	05	Security Alerts, Advisories, and Directives	Main	[1]	Reference	List of personnel to which security alerts, advisories, and directives should be disseminated.	Center CIOs, Center CISOs, OCSOs, other security personnel and stakeholders (e.g., ISOs, ISSOs).	Center CIOs, Center CISOs, OCSOs, other security personnel and stakeholders (e.g., ISOs, ISSOs).	Center CIOs, Center CISOs, OCSOs, other security personnel and stakeholders (e.g., ISOs, ISSOs).
SI	06	Security Functionality Verification	Main	[1]	Selection	System transitional states verified for correct operation of the security functions.			(1) Upon system startup and restart (2) Upon command by user with appropriate privilege. (3) At least every 24 hours
SI	06	Security Functionality Verification	Main	[2]	Selection	Actions when anomalies are detected in transitional states.			Automatically notify the system administrator
SI	07	Software and Information Integrity	E 1	[1]	Frequency	Assessment of software and information integrity through scans.		ISO-defined frequency commensurate with risks.	ISO-defined frequency commensurate with risks.
SI	07	Software and Information Integrity	E 4	[1]	Reference	Information system components requiring tamper-evident packaging.			
SI	07	Software and Information Integrity	E 4	[2]	Selection	Scenarios where tamper-evident packaging for information system components must be used.			

ITS Handbook (ITS-HBK-2810.14-01) -
System and Information Integrity -

Family	#	Name	Section	Parameter	Type	Description	Low	Moderate	High
SI	11	Error Handling	Main	[1]	Reference	List of sensitive or potentially harmful information.		(1) PII (Personally Identifiable Information) (2) UserID (3) Passwords (4) Other sensitive information specific to the information system	(1) PII (2) UserID (3) Passwords (4) Other sensitive information specific to the information system
SI	13	Predictable Failure Prevention	Main	[1]	Reference	List of information system components where protection takes into consideration mean time to failure within specific environments of operation.			
SI	13	Predictable Failure Prevention	E 1	[1]	Percentage	Threshold for decommissioning systems approaching mean time to failure.			
SI	13	Predictable Failure Prevention	E 2	[1]	Time Period	Limits on process execution without supervision.			
SI	13	Predictable Failure Prevention	E 3	[1]	Frequency	Manual initiation of transfer between active and standby information systems.			
SI	13	Predictable Failure Prevention	E 3	[2]	Time Period	Limit on exceeding mean time to failure before transfer between active and standby information systems is manually initiated.			
SI	13	Predictable Failure Prevention	E 4	[1]	Time Period	Failover time between successful and transparent assumption of roles by standby systems.			
SI	13	Predictable Failure Prevention	E 4	[2]	Selection	Action upon failure detection.			
SI	13	Predictable Failure Prevention	E 4	[2] [1]	Reference	Alarm activated in case of failure detection.			